Prediction of DoS Attacks in External Communication for Self-driving Vehicles Using A Fuzzy Petri Net Model

Khattab M. Ali Alheeti
School of Computer Sciences and Electronic Engineering
University of Essex, Colchester, United Kingdom
University of Anbar, College of Computer – Anbar, Iraq
kmali@essex.ac.uk

Anna Gruebler, Klaus D. McDonald-Maier, †Anil Fernando
School of Computer Sciences and Electronic Engineering, University of Essex
Colchester, United Kingdom
†Centre for Vision, Speech and Signal Processing, University of Surrey
contact@annagruebler.com, kdm@essex.ac.uk, w.fernando@surrey.ac.uk

***Abstract*—In this paper we propose a security system to protect external communications for self-driving and semi self-driving cars. The proposed system can detect malicious vehicles in an urban mobility scenario. The anomaly detection system is based on fuzzy petri nets (FPN) to detect packet dropping attacks in vehicular ad hoc networks. The experimental results show the proposed FPN-IDS can successfully detect DoS attacks in external communication of self-driving vehicles.**

***Index Terms*—Security, self-driving cars, platoon, IDS, FPN.**

I. Introduction

Self-driving vehicles can have positive implications for our society, such as reducing the number of accidents on busy roads and reducing the amount of pollution [1]. Communication between vehicles and roadside units (RSUs) lead to considered a significant progress in the world of cars because it can provide increased driving comfort, enhanced traffic safety and raise economic and ecological efficiency. These technologies are called vehicular ad hoc networks (VANETs): car to car communication (C2C) and car to RSU communication (C2R). VANETs possess unique characteristics (includeing the operating environment) which make them more vulnerable to attacks [2].

Self-driving cars send cooperative awareness messages (CAMs) via wireless channels to inform other vehicles about the status in their zone. CAMs could be sent to predict the state of vehicles in order to avoid risks. An additional advantage of self-driving vehicles is the ability to avoid traffic jams and finding better roads by using information from the VANET. This is realized through the platoon behavior of the vehicles in the network: vehicles in a network are travelling in a convoy-like formation. In our work we use ad hoc on-demand distance vectors (AODV), which are a type of reactive routing protocols [2].

In previous research, Fuzzy Petri Nets (FPNs) have been shown to enhance the security system used wireless ad hoc networks [3]. FPN combined with a mathematical model and a set of methodologies [3] provides control and reliability in the real word. FPNs have a number of applications: control, scheduling, communication, decision making and classification. In our research, we utilize the FPN for classification between normal and abnormal communications. Pouyan et al. proposed a security system to protect routing protocols such as the AODV in mobile ad hoc networks (MANETs) [3]. The proposed system was based on the fuzzy Petri net and was a robust system to secure control data and notification messages exchanged between nodes. Han et al. proposed a novel security protocol to protect vehicle-to-mobile communication in VANETs based on MVSec. It ensures security between vehicles and phones without any pre-shared secure key [3]. The proposed system has a vital role in enhancing performance for the routing protocol AODV which has been used in their simulation environment. Ali et al. proposed an intrusion detection system based on artificial neural networks to detect malicious behaviour in VANETs [5]. The proposed security system has the ability to detect and identify attacks, such as black hole attacks. Chaudhary et al. proposed an intrusion detection system based on fuzzy logic to secure MANETs [6]. It can detect dropping attacks as well as isolated malicious vehicles based on their IP.

Here, we propose a system based on the FPN to deliver an intelligent security system that predicts attacks on the external communications of autonomous and semi-autonomous vehicles. Petri nets are used in many applications. However rapid industrial development prevents adoption of the petri nets because this technology is unable to perform certain tasks. This encourage researchers to combine petri nets with fuzzy logic to create a new technique called FPN [7].

II. Proposed Intrusion Detection System Based on Fuzzy Petri Nets

The proposed intrusion detection system based on fuzzy petri nets is based on a number of features, which have been extracted from the trace file. It was generated from network simulator-2 (NS2). These features are considered fuzzy parameters for the proposed system. In this paper, we built an intelligent security system which employed FPN in detecting malicious vehicles based on parameters that reflect vehicles behaviour on roads.

A. Mobility Model for Self-driving vehicles

The proposed IDS uses two tools to generate a real environment for self-driving and semi self-driving vehicles. These tools are: Simulation of Urban Mobility Model (SUMO) and MObile VEhicles (MOVE). The IDS generates to create two types of scenarios: normal and malicious behaviour. Each scenario has 70 vehicels with different number of malicious vehicles. We extracted some parameters from VANETs that describe the normal and abnormal behaviours of self-driving vehicles. The FPN-IDS used 9 rules to achieve this. The following is an example rule:

If PDR is "Low" and DPR is "Medium" then VL shift is "Low"

B. Intelligent Security System

The only method of identifying malicious behaviour is sending and receiving the CAMs over a shared communication channel between vehicles and their RSUs. Any security system proposed to protect the routing protocol has two concerns: (1) secure transmitted data packets or control packets from a vehicle to another (point to point), (2) secure whole packets transmitted between vehicles in that zone. Fundamentally, an IDS is capable

of three types of intrusion detections: 1) anomaly, 2) misuse and 3) specification. Anomaly detection is utilized in secure external communication for VANETs. This type of detection is based on pre-knowledge. It can identify novel attacks, but it has one problems i.e. the high rate of false alarms. Figure 1 shows the architecture of the proposed IDS. Misuse detection can detect infiltration through known attack signatures by comparing traffic patterns. While, specification based detection identifies attacks when deviations from a norm occur. It is based on manually developed specifications that capture legitimate behaviour.

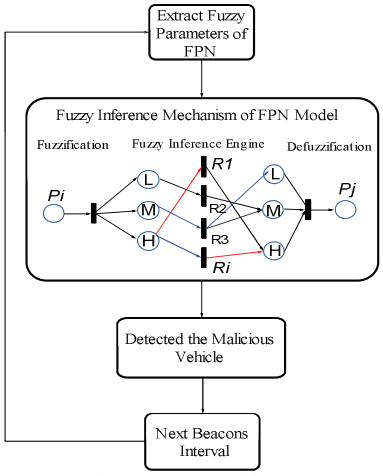

Fig. 1: System Architecture

The system first generates the fuzzy parameters. They are then fuzzified and processed based on the inferencing engine utilizing nine fuzzy rules. The output is defuzzified and is compared with a threshold to predict normal or abnormal behaviour.

III. Results

We utilized NS2 to evaluate the performance of the proposed IDS. The IDS heavily depends on features which have been extracted from the trace file. These features are considered fuzzy parameters for the FPN. The features are: Packet Delivery Ratio (PDR) and Drop Packet Ratio (DPR). We calculated the classification rate and the rate of four types of alarms using the proposed system. The results are shown in Table 1:

TABLE 1 CLASSIFICATION RATE

Class	Accuracy	P-value	Standard Deviation
Normal	58.33%		
Abnormal	100%	0.000107	8.3120
Threshold	0.66		

Alarm	Accuracy	Alarm	Accuracy
True Positive (TP)	72.22%	False Positive (FP)	0%
True Negative (TN)	100%	False Negative (FN)	27.78%

We evaluated the performance metrics of VANETs with or without the FPN-IDS for self-driving and semi self-driving vehicles. The metrics are PDR, Average End-to-End Delay and Average Throughput, Table 2 shows the performance metrics of FPN-IDS:

TABLE 2 PERFORMANCE METRICS

Performance Metrics	VANETs with FPN-IDS	VANETs without FPN-IDS
PDR	98.31%	32%
Throughput	79.98%	31.07%
End-to-End Delay	213.17s	8.28s

The accuracy of detection and alarms heavily depends on the value of the threshold [6]. We tested the proposed system with different values of threshold to calculate the accuracy of detection rate and false positive rate in order to select the optimal threshold value. In our research the threshold is set at 0.42 because the verity level or increasing detection rate lies between 0.38 and 0.48. The proposed system is evaluated under different conditions: The total number of generated packets is 2368 packets in two scenarios, while the number of received packets is 2115 in VANETs with IDS. Thus the total number of dropped packets is 254 while 751 packets are received and total number of dropped packets is 1618 in VANETs without FPN-IDS.

IV. Discussion

We can observe that the FPN-IDS can enhance the security of VANETs. Taking into account the number of received and dropped packets, we can easily see the important role of IDS in VANETs. The output metrics detect abnormal behaviour in the range of 0.37 to 0.25. When we set the threshold value at 0.42, we obtained 0% of the false rate as well as 100% detection rate. Comparing these results with previous research [6] where FPN were not employed the false rate ranged between 0.05% and 1.6% [6]. The FPN-IDS can be extended to design other IDS which can be used to identify many other types of attacks.

V. Conclusion

In this paper, we propose anomaly FPN-IDS based on parameters calculated from the trace file. The proposed security system has the ability to identify the attacking vehicle in the VANET. The FPN-IDS is considered a novel security system to protect VANETs because this is the first time an FPN has been used in VANETs. The FPN-IDS can provide sufficient security to external communication of self-driving vehicles and has the ability to detect external and internal attacks launched at any time. Our proposed work can also isolate malicious vehicles with high detection rate and low false alarms. In future work, we will attempt to utilize the IDS on VANETs based on Time Division Multiple Access (TDMA) to generate a clustering model. A clustering based TDAM architecture provides VANETs, scalability and fault tolerance and as a result gives more efficient use of VANETs resources.

References

[1] T. Lomax David and S. Turner, 2010 Annual Urban Mobility Report. Technical report, Texas Transportation Institute, 2010.

[2] Q. Fengzhong, W. Zhihui, W. Fei-Yue, and C. Woong, "A Security and Privacy Review of VANETs," IEEE Transactions On Intelligent Transportation Systems, ISSN 1524-9050, pp. 1-12, 2015.

[3] H. Jun, L. Yue-Hsun, P. Adrian and B. Fan," MVSec: secure and easy-to-use pairing of mobile devices with vehicles,"ACM conference on Security and Privacy in Wireless and Mobile Networks, 2014.

[4] A. Pouyan, M. Tabari, " FPN-SAODV: using fuzzy petri net for securing AODV routing protocol in mobile ad hoc network," International Journal of Communication Systems, no. 10. 1002, 2015.

[5] K. Ali Alheeti, A. Gruebler, K. D. McDonald-Maier, " An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars", 12th IEEE CCNC, pp. 916–921,2015.

[6] A. Chaudhary, V. Tiwar, A. Kumar, " Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks," IEEE Advance Computing Conference, pp. 256 - 261, 2014.

[7] T. Murata, "Petri Nets: Properties, Analysis and Applications," Proceedings of the IEEE. Vol. 77, No. 4, 1989.